

**U.S. Department of Commerce
U.S. Patent and Trademark Office**



**Privacy Impact Assessment
for the
Information Delivery Product (IDP)**

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

- ☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS

Digitally signed by CATRINA PURVIS

Date: 2020.08.31 13:22:42 -04'00'

08/30/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

U.S. Department of Commerce Privacy Impact Assessment Information Delivery Product (IDP)

Unique Project Identifier: PTOC-003-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) *Whether it is a general support system, major application, or other type of system*

Information Delivery Product (IDP) is a Major Application within the United States Patent and Trademark Office (USPTO).

(b) *System location*

IDP resides at the USPTO facilities located in Alexandria, Virginia.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

IDP interconnects with the following systems:

- Network and Security Infrastructure System (NSI)
- Corporate Administrative Office System (CAOS)
- Enterprise Software Services (ESS)
- Enterprise Unix Services (EUS)
- Enterprise Windows Services (EWS)
- Service Oriented Infrastructure System (SOI)
- Consolidated Financial System (CFS)
- Enterprise Desktop Platform (EDP)
- Patent Capture and Application Processing System –Examination Support (PCAPS-ES)
- Agency Administrative Support System (AASS)
- Fee Processing Next Generation (FPNG)
- Patent Trial and Appeal Board End to End (PTAB-E2E)
- Enterprise Records Management and Data Quality System (ERMDQS)
- Corporate Web Systems CWS)
- Database Services (DBS)
- U.S. Department of Agriculture (USDA) National Finance Center (NFC)
- U.S. Treasury HR Connect

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*

IDP provide users access to USPTO financial-related documents to support the decision-making activities of managers and analysts. The system provides an interface for users to access the database, generate reports and have the ability to visualize the data.

EDW: is a USPTO system providing access to integrated USPTO data through various tools in support of not only reporting and visualizing but also analytics used in decision-making across USPTO.

EL4FMS: is an automated information system (AIS) that provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. EL4FMS also supports users' business operations by providing access via FPNG to

various financial documents relating to their FPNG account.

FEDMT: FEDMT is a database/user interface solution utilizing the Oracle Application Express (APEX) product to build small applications to support Financial Reference data as well as financial administrative tasks.

(e) *How information in the system is retrieved by the user*

Information is retrieved via the Financial Enterprise Data Management Tools interface.

(f) *How information is transmitted to and from the system*

Communications utilize a minimum of TLS 1.1 with FIPS 140-2 compliant algorithms to provide transmission confidentiality and integrity for all connections outside the system boundary. The externally-facing VIPs supporting IDP are configured to only support TLS 1.1 and TLS 1.2.

(g) *Any information sharing conducted by the system*

IDP supports users' business operations by providing access via FPNG to various financial documents relating to their FPNG account..

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

The USPTO collects customer financial information for fee processing under 35 U.S.C. 2 and 41 and 15 U.S.C.1113, as implemented in 37 CFR 1.16–1.28, 2.6–2.7, and 2.206–2.209. The authority for the USPTO employees' PII in IDP is E.O. 9397.

(i) *The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

IDP is categorized as a Moderate system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- ☐ This is a new information system.
- ☐ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character	<input type="checkbox"/>

Management Changes				of Data	
j. Other changes that create new privacy risks (specify):					

- ☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.
- ☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).
- ☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	<input checked="" type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
b. Taxpayer ID	<input checked="" type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input checked="" type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input type="checkbox"/>				
n. Other identifying numbers (specify):					
<p>*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:</p> <p>IDP maintains Social Security Numbers (SSNs) of USPTO employees for human resources reporting purposes. The source systems from which it receives SSNs are the U.S Department of Agriculture (USDA) National Finance Center (NFC) and the USPTO Patent Capture and Application Processing System – Examination Support (PCAPS-ES) Patent Application Location Monitoring (PALM) Infrastructure System (INFRA).</p>					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input checked="" type="checkbox"/>	o. Financial Information	<input checked="" type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input checked="" type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input checked="" type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input checked="" type="checkbox"/>	m. Education	<input checked="" type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	<input checked="" type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	f. Salary	<input checked="" type="checkbox"/>	j. Proprietary or Business	<input type="checkbox"/>

				Information	
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input checked="" type="checkbox"/>		
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input type="checkbox"/>
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input checked="" type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application	<input type="checkbox"/>				
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Data is pulled from PTO authoritative sources, which have the responsibility for data accuracy.

2.4 Is the information covered by the Paperwork Reduction Act?

<input type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
<input checked="" type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	<input type="checkbox"/>	For administering human resources programs	<input checked="" type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify):			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The Delivery Product integrates existing data from multiple USPTO sources and HR data from the U.S Department of Agriculture (USDA) National Finance Center (NFC). It makes data comparisons available for analysis.

This information is collected to support the decision-making activities of managers and analysts in the PTO's business areas to analyze USPTO data. Specifically, the information will provide managers and analysts the ability to analyze business processes, resource use and needs, and other facets of the business and provide the USPTO with the means of performing at a more efficient, accurate, and cost effective level.

One subject area of the IDP is the Human Resources Subject Area (HRSA). HRSA is a reporting mechanism for HR to allow authorized users (both within OHR and for managers throughout PTO) to run reports, such as staff listings, within Grade Increases projections, employee counts, accession/separation lists, etc. The data warehouse (which stores USDA NFC, U.S Treasury HR Connect, and general employee locator content) in conjunction with the Business objects reporting tool, allows for the dissemination of information to authorized users.

- 5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The potential danger in the BII being compromised is the potential for sharing of information that is required to be held in confidence for a specified period of time per statute and regulation, e.g., 35 USC 122 and 37 CFR 1.211. All end-users and administrators of the BDR system have a valid need-to-know access to the system, and undergo the USPTO Annual IT Security Awareness Training provided by the agency. This training covers proper information handling, retention, and disposal at an enterprise level, which is applicable to all information systems.

Section 6: Information Sharing and Access

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ The PII/BII in the system will not be shared.

- 6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: USPTO</p> <ul style="list-style-type: none"> • Consolidated Financial System (CFS) <ul style="list-style-type: none"> o Momentum • Corporate Administrative Office System (CAOS) <ul style="list-style-type: none"> o Web Time and Attendance (WebTA) • Employee Relations/Labor Relations Case Management System (ERLRCMS) • Fee Processing Next Generation (FPNG) • Planning Budgeting Products (PBP) <ul style="list-style-type: none"> o Corporate Planning Tool (CPT) • Patent Capture and Application Processing System – Examination Support (PCAPS-ES)
-------------------------------------	--

	<ul style="list-style-type: none"> o Patent Application Location Monitoring (PALM) Examination and Post-Examination (EXPO) o Patent Application Location Monitoring (PALM) Infrastructure System (INFRA) • Patent Trial and Appeal Board End to End (PTAB E2E) • Reasonable Accommodation Case Management System (RACMS) <p>External Systems:</p> <ul style="list-style-type: none"> • U.S. Department of Agriculture (USDA) National Finance Center (NFC) • U.S. Treasury HR Connect <p>The information transmitted between the systems is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) and the Enterprise Monitoring and Security Operations (EMSO) systems.</p>
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). Individuals may be notified that their PII/BII is collected, maintained, or disseminated by the primary application ingress system.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide	Specify why not: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). These front end

	PII/BII.	systems provide this functionality for the data that is being collected. IDP has no authorization to decline any type of information since it's owned by the primary application
--	----------	--

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: : IDP receives PII/BII indirectly from application systems (i.e front end systems). These front end systems provide this functionality for data that is being collected.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected. IDP has no authorization to review/update any type of information since it's owned by the primary application.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to PII/BII is being monitored and tracked through audit logs.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>09/19/2019</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

- 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Management Controls:

The USPTO uses the Life Cycle review process to ensure that management controls are in place for the IDP. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational, and technical controls that are in place, and planned during the operation of the enhanced system. Additional management controls include performing national agency check on all personnel, including contractor staff.

Operational Controls:

Operational controls include securing all hardware associated with this system in the USPTO Data Center. The Data Center is controlled by access card entry, and manned by a uniformed guard service to restrict access to the servers, their operation systems and databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions” (2) Physical terminal identification; (3) Database UserID; (4) restricted data display, as required; and (5) restricted access.

Technical Controls:

Technical controls include password authentication (userid and passwords). At the client PCs’, access is managed through a password authentication (userid and passwords) based on certification in a Financial Access Request Management (FARM) system. Requests are approved first by the user’s supervisor, then require additional approval from Human Resources based on a justification of need.

Technical controls include password authentication (userid and passwords). At the client PCs’, access is managed through a password authentication (userid and passwords) based on certification on a Financial Application Security Registration form. The security form must be signed by a supervisor, and requires additional approval from Human Resources based on a justification of need.

Section 9: Privacy Act

- 9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>): Existing System of Records notices cover the information pulled from other systems residing in the Enterprise Data Warehouse. These include: • Commerce/PAT-TM 3, Employee Production records; • Commerce/PAT-TM-7, Patent Application Files; • Commerce/PAT-TM 10, Patent Deposit Accounts System; and • Commerce/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on (date).
<input type="checkbox"/>	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. (*Check all that apply.*)

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: GRS 4:3:031 records schedule
<input type="checkbox"/>	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. (*Check all that apply.*)

Disposal			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.
(*The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.*)

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious

	adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.
(Check all that apply.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Social Security Number (SSN), name, gender, age, race/ethnicity, home/business address, email address, telephone number, financial information
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: Collectively, the number of records maintained generate an enormous amount of PII and a breach in such large numbers of individual PII must be considered in the determination of the impact level.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: Combination of name, SSN, and financial information may be more sensitive.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: PII is stored to support the decision making activities of managers and analysts in the PTO's business areas to analyze USPTO data.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Due to obtaining PII, necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

IDP resides in USPTO East production environment. Access to IDP is very limited and controlled by the IDP PM team. IDM accounts must be created by Operations for new accounts requested by members of the IDP PM team. Data is protected in transit through TLS 1.2. Administrative access to the back-end is limited to trusted individuals on the development team. Access to the IDP is controlled through RBAC enforcement. The correspondence related to non-published applications are made public when the application is made public (typically after a period of 18 months). Given the limited access under this category, the threat of BII leakage is very low. Access to the user interface is not exposed to the public internet and only kept internally within the USPTO network.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.